

Κεφάλαιο 1

Πρότυπα

Στο κεφάλαιο αυτό εισάγουμε την έννοια του προτύπου πάνω από δακτύλιο.

1.1 Ορισμοί και Παραδείγματα

Παραδοχές Στο βιβλίο αυτό θα κάνουμε τις εξής παραδοχές.

- Χρησιμοποιούμε προσθετικό συμβολισμό για αβελιανές ομάδες. Δηλαδή αν M είναι μια αβελιανή ομάδα, τότε η πράξη της M θα συμβολίζεται με $M \times M \rightarrow M, (m_1, m_2) \rightarrow m_1 + m_2$. Το ουδέτερο στοιχείο της M θα συμβολίζεται με 0_M ή απλά 0 .
- Κάθε δακτύλιος περιέχει μοναδιαίο στοιχείο. Το μοναδιαίο στοιχείο ενός δακτυλίου R συμβολίζεται με 1_R ή απλά 1 . Επίσης υποθέτουμε ότι $1_R \neq 0_R$, δηλαδή ότι $R \neq 0$. Συνεπώς όταν θεωρούμε τους δακτυλίους $\mathbb{Z}_n$ θα υποθέτουμε ότι $n > 1$.
- Κάθε ομομορφισμός δακτυλίων διατηρεί τα μοναδιαία στοιχεία, δηλαδή αν $f: R \rightarrow S$ είναι ομομορφισμός δακτυλίων, τότε πέρα από τις σχέσεις $f(r_1 + r_2) = f(r_1) + f(r_2)$ και $f(r_1 r_2) = f(r_1) f(r_2)$, όπου $r_1, r_2 \in R$, ικανοποιείται και η σχέση $f(1_R) = 1_S$.
- Όταν λέμε ιδεώδες ενός δακτυλίου εννοούμε αριστερό ιδεώδες, δηλαδή ένα ιδεώδες I ενός δακτυλίου R είναι ένα μη κενό σύνολο $I \subseteq R$ τέτοιο ώστε για κάθε $a, b \in I, r \in R$ έχουμε $a - b \in I$ και $ra \in I$.
- Με $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ συμβολίζουμε αντίστοιχα το σύνολο των θετικών ακεραίων, ακεραίων, ρητών, πραγματικών και μιγαδικών αριθμών. Το κενό σύνολο συμβολίζεται με $\emptyset$.

1.1.1 Ορισμός Έστω R ένας δακτύλιος. Μια αβελιανή ομάδα M εφοδιασμένη με μια απεικόνιση

$$R \times M \ni (r, m) \mapsto r \cdot m \in M$$

ονομάζεται **R - πρότυπο** ή **πρότυπο πάνω από το R** αν ισχύουν οι εξής ιδιότητες

- (i) $r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m$ για κάθε $r_1, r_2 \in R$, $m \in M$
- (ii) $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$ για κάθε $r_1, r_2 \in R$, $m \in M$
- (iii) $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$ για κάθε $r \in R$, $m_1, m_2 \in M$
- (iv) $1_R \cdot m = m$ για κάθε $m \in M$.

Στον προηγούμενο ορισμό, θα ονομάζουμε την απεικόνιση $R \times M \rightarrow M$ τον **εξωτερικό πολλαπλασιασμό** του R -πρότυπου M . Στα παρακάτω θα γράφουμε rm στη θέση του $r \cdot m$.

1.1.2 Παραδείγματα

1. Έστω k ένα σώμα. Κάθε k -διανυσματικός χώρος είναι k -πρότυπο. Μάλιστα οι έννοιες k -διανυσματικός χώρος και k -πρότυπο ταυτίζονται.
2. Κάθε αβελιανή ομάδα M είναι $\mathbb{Z}$ -πρότυπο με εξωτερικό πολλαπλασιασμό $\mathbb{Z} \times M \rightarrow M$, $(r, m) \mapsto rm$, που ορίζεται από τη σχέση

$$rm = \begin{cases} m + \dots + m & (r \text{ φορές}), \text{ αν } r > 0 \\ 0, & \text{αν } r = 0 \\ -((-r)m), & \text{αν } r < 0, \end{cases}$$

όπου $r \in \mathbb{Z}$ και $m \in M$. Εύκολα βλέπουμε ότι οι έννοιες αβελιανή ομάδα και $\mathbb{Z}$ -πρότυπο ταυτίζονται.

3. Κάθε ιδεώδες I δακτυλίου R είναι R -πρότυπο με εξωτερικό πολλαπλασιασμό $R \times I \rightarrow I$, $(r, a) \mapsto ra$. Ειδικά, κάθε δακτύλιος R είναι R -πρότυπο.
4. Έστω I ένα ιδεώδες ενός δακτυλίου R . Η αβελιανή ομάδα R/I είναι R -πρότυπο με εξωτερικό πολλαπλασιασμό $R \times R/I \rightarrow R/I$ που ορίζεται από

$$r(a + I) = ra + I,$$

όπου $a, r \in R$. Η σχέση αυτή είναι καλά ορισμένη, γιατί αν $a + I = a' + I$ και $r \in R$, τότε $a - a' \in I$ και άρα $r(a - a') \in I$, δηλαδή $ra - ra' \in I$ που σημαίνει ότι $ra + I = ra' + I$. Η επαλήθευση των αξιωμάτων του Ορισμού 1.1.1 είναι εύκολη.

5. Έστω R ένας δακτύλιος. Ο δακτύλιος $R[x]$ των πολυωνύμων στη μεταβλητή x με συντελεστές από το R είναι ένα R -πρότυπο με εξωτερικό πολλαπλασιασμό $R \times R[x] \rightarrow R[x]$, $(r, f(x)) \mapsto rf(x)$.
6. Έστω V ένας k -διανυσματικός χώρος, όπου το k είναι σώμα, και $\alpha : V \rightarrow V$ μια γραμμική απεικόνιση. Αν

$$f = f_0 + f_1 x + \dots + f_n x^n \in k[x]$$

είναι ένα πολυώνυμο, τότε με $f(a):V \rightarrow V$ συμβολίζουμε τη γραμμική απεικόνιση

$$f_0 1_V + f_1 \alpha + \dots + f_n \alpha^n,$$

όπου $1_V:V \rightarrow V$ είναι η ταυτοτική απεικόνιση, $1_V(v)=v$, και $\alpha^k:V \rightarrow V$ είναι η σύνθεση $\alpha \circ \dots \circ \alpha$ (k φορές). Το V είναι ένα $k[x]$ -πρότυπο με εξωτερικό πολλαπλασιασμό

$$k[x] \times V \rightarrow V, (f, v) \mapsto fv = f(\alpha)(v).$$

Αφήνουμε την απόδειξη ως άσκηση.

7. Έστω R ένας δακτύλιος. Το σύνολο $M_{m \times n}(R)$ των $m \times n$ πινάκων με στοιχεία από το R είναι ένα R -πρότυπο με πρόσθεση τη συνήθη πρόσθεση πινάκων και με εξωτερικό πολλαπλασιασμό $R \times M_{m \times n}(R) \rightarrow M_{m \times n}(R)$, $(r, A) \mapsto rA$, όπου $rA = (ra_{ij})$ αν $A = (a_{ij})$.
8. Θεωρούμε το δακτύλιο $M_n(R)$ των $n \times n$ πινάκων με στοιχεία από ένα δακτύλιο R . Η αβελιανή ομάδα $M_{n \times 1}(R)$ είναι ένα $M_n(R)$ -πρότυπο με εξωτερικό πολλαπλασιασμό $M_n(R) \times M_{n \times 1}(R) \rightarrow M_{n \times 1}(R)$, $(A, X) \mapsto AX$, όπου AX είναι το γινόμενο των πινάκων A, X .
9. Έστω M μια αβελιανή ομάδα και $R = \text{End}M$ το σύνολο των ομομορφισμών ομάδων $M \rightarrow M$. Το R είναι ένας δακτύλιος με πρόσθεση που ορίζεται από τη σχέση $(f + g)(m) = f(m) + g(m)$ και πολλαπλασιασμό που ορίζεται από τη σύνθεση συναρτήσεων $(fg)(m) = f(g(m))$, όπου $f, g \in \text{End}M$, $m \in M$. Το M γίνεται R -πρότυπο με εξωτερικό πολλαπλασιασμό $R \times M \rightarrow M$, $(f, m) \mapsto f(m)$.

1.1.3 Πρόταση Έστω M ένα R -πρότυπο. Τότε έχουμε

- (i) $0_R m = 0_M$ για κάθε $m \in M$
- (ii) $r 0_M = 0_M$ για κάθε $r \in R$
- (iii) $(-r)m = r(-m) = -rm$ για κάθε $r \in R$, $m \in M$.

Απόδειξη (i) Έχουμε $0_R + 0_R = 0_R \Rightarrow (0_R + 0_R)m = 0_R m \Rightarrow$

$0_R m + 0_R m = 0_R m$. Από το νόμο της διαγραφής που ισχύει στην ομάδα M παίρνουμε $0_R m = 0_M$.

(ii) Έχουμε $0_M + 0_M = 0_M \Rightarrow r(0_M + 0_M) = r0_M \Rightarrow r0_M + r0_M = r0_M \Rightarrow r0_M = 0_M$.

(iii) Από το (ii) παίρνουμε $r(m + (-m)) = r0_M = 0_M \Rightarrow rm + r(-m) = 0_M$
 και άρα $r(-m) = -(rm)$. Από το (i) έχουμε
 $(r + (-r))m = 0_R m = 0_M \Rightarrow rm + (-r)m = 0_M$. Άρα $(-r)m = -(rm)$. $\square$

Στο παρακάτω θα χρησιμοποιούμε τις σχέσεις της Πρότασης 1.1.3 χωρίς ιδιαίτερη μνεία.

Τονίζουμε ότι σ' ένα R -πρότυπο M είναι δυνατό να ισχύει $rm = 0_M$ ακόμα και αν $r \neq 0_R$ και $m \neq 0_M$. Για παράδειγμα, στο $\mathbb{Z}$ -πρότυπο $\mathbb{Z}_n$ έχουμε $n[a] = [na] = [0]$ για κάθε $[a] \in \mathbb{Z}_n$.

1.1.4 Ορισμός Έστω M ένα R -πρότυπο. Ένα υποσύνολο $N \subseteq M$ ονομάζεται **R -υποπρότυπο** του M αν το N είναι υποομάδα της M και για κάθε $r \in R$, $a \in N$ έχουμε $ra \in N$.

Παρατηρούμε ότι αν το N είναι υποπρότυπο του M , τότε το N είναι R -πρότυπο ως προς τον εξωτερικό πολλαπλασιασμό $R \times N \rightarrow N, (r, a) \mapsto ra$, όπου $R \times M \rightarrow M, (r, m) \mapsto rm$ είναι ο εξωτερικός πολλαπλασιασμός του M . Θα χρησιμοποιούμε το συμβολισμό $N \leq M$ για να δηλώσουμε ότι το N είναι υποπρότυπο του M .

1.1.5 Λήμμα Έστω M ένα R -πρότυπο και $N \subseteq M$ ένα μη κενό υποσύνολο του M . Τότε το N είναι υποπρότυπο του M αν και μόνο αν για κάθε $a, b \in N$, $r \in R$ έχουμε $a - b \in N$ και $ra \in N$.

Απόδειξη Έπεται άμεσα από το γεγονός ότι ένα μη κενό υποσύνολο N μιας ομάδας M είναι υποομάδα αν και μόνο αν $a - b \in N$ για κάθε $a, b \in N$. $\square$

1.1.6 Παραδείγματα

1. Έστω R ένας δακτύλιος. Τα R -υποπρότυπα του R είναι τα ιδεώδη του R .
2. Τα $\mathbb{Z}$ -υποπρότυπα μιας αβελιανής ομάδας είναι οι υποομάδες της.
3. Έστω k ένα σώμα. Τα k -υποπρότυπα ενός k -διανυσματικού χώρου είναι οι υπόχωροί του.
4. Έστω R ένας δακτύλιος, n ένας μη αρνητικός ακέραιος και $R_n[x] = \{f(x) \in R[x] \mid \deg f(x) \leq n\}$, όπου $\deg f(x)$ είναι ο βαθμός του $f(x)$. (Σημείωση: δεχόμαστε ότι ο βαθμός του μηδενικού πολυ-

ωνόμου $f(x)=0$ είναι $\deg f(x)=-\infty$ και $-\infty < n$ για κάθε n). Τότε $R_n[x] \leq R[x]$.

5. Έστω V ένας k -διανυσματικός χώρος, όπου το k είναι σώμα, και $\alpha: V \rightarrow V$ μια γραμμική απεικόνιση. Στο Παράδειγμα 1.1.2 6, είδαμε ότι το V είναι ένα $k[x]$ -πρότυπο. Ένα υποσύνολο U του V είναι $k[x]$ -υποπρότυπο του V αν και μόνο αν το U είναι υπόχωρος του V τέτοιος ώστε $\alpha(U) \subseteq U$.

Πράγματι, έστω ότι το U είναι $k[x]$ -υποπρότυπο του V . Τότε για κάθε $u, u' \in U$ και $r \in k$ έχουμε $u - u' = 1_V u + (-1_V) u' \in U$ και $ru = (r1_V)(u) \in U$. Άρα το U είναι υπόχωρος του V . Επίσης, για κάθε $u \in U$ έχουμε $xu \in U$, δηλαδή $\alpha(u) \in U$.

Αντίστροφα, έστω ότι το U είναι υπόχωρος του V τέτοιος ώστε $\alpha(U) \subseteq U$. Αν $u \in U$, τότε από $\alpha(u) \in U$ έπεται ότι $(rx^n)u = r\alpha^n(u) \in U$ για κάθε $r \in k$ και $n \geq 0$. Επειδή το U είναι υπόχωρος έχουμε $f(x)u \in U$ για κάθε $f(x) \in k[x]$. Άρα το U είναι $k[x]$ -υποπρότυπο του V σύμφωνα με το Λήμμα 1.1.5.

Αν το M είναι R -πρότυπο, τότε το σύνολο $\{0_M\}$ είναι ένα υποπρότυπο του M που θα το ονομάζουμε το **τετριμμένο ή μηδενικό** υποπρότυπο και θα το συμβολίζουμε με 0 .

Από το Λήμμα 1.1.5 έπεται ότι η τομή μιας μη κενής οικογένειας R -υποπροτύπων ενός R -προτύπου είναι ένα R -πρότυπο. Η απόδειξη αφήνεται ως άσκηση.

1.1.7 Ορισμός Έστω $X \neq \emptyset$ ένα υποσύνολο του R -προτύπου M . Το υποπρότυπο του M που **παράγεται** από το X είναι η τομή όλων των υποπροτύπων του M που περιέχουν το X . Θα το συμβολίζουμε με (X) .

1.1.8 Πρόταση Έστω $X \neq \emptyset$ ένα υποσύνολο του R -προτύπου M . Τότε

$$(X) = \left\{ \sum_{i=1}^n r_i x_i \mid n \in \mathbb{N}, r_i \in R, x_i \in X \right\}.$$

Απόδειξη Έστω A το δεξί μέλος της παραπάνω ισότητας. Ισχύει $A \subseteq (X)$. Πράγματι, έστω N ένα υποπρότυπο του M που περιέχει το X .

Τότε $x_i \in X \Rightarrow x_i \in N \Rightarrow r_i x_i \in N$ για κάθε $r_i \in R$. Άρα $\sum_{i=1}^n r_i x_i \in N$. Συ-

νεπώς $\sum_{i=1}^n r_i x_i \in (X)$. Ισχύει $(X) \subseteq A$. Πράγματι, από το Λήμμα 1.1.5

έπεται ότι το A είναι υποπρότυπο του M που περιέχει το X . Το (X) ως τομή τέτοιων προτύπων θα περιέχεται στο A . $\square$

Κατ' αναλογία με τους διανυσματικούς χώρους, αν το $X \subseteq M$ έχει την ιδιότητα $(X) = M$, θα λέμε ότι το X **παράγει** το M ή ότι το M **παράγεται** από το X ή ότι το X είναι ένα **σύνολο γεννητόρων** του M .

Αν το $X \subseteq M$ είναι πεπερασμένο, $X = \{x_1, \dots, x_m\}$, θα συμβολίζουμε το (X) με $(x_1, \dots, x_m)$ ή $Rx_1 + \dots + Rx_m$.

1.1.9 Ορισμός (i) Ένα R -πρότυπο M λέγεται **πεπερασμένα παραγόμενο** αν υπάρχει πεπερασμένο υποσύνολο $X \subseteq M$ τέτοιο ώστε $(X) = M$.

(ii) Ένα R -πρότυπο M λέγεται **κυκλικό** αν υπάρχει $m \in M$ τέτοιο ώστε $M = (m)$.

Για παράδειγμα, τα κυκλικά k -υποπρότυπα ενός μη μηδενικού k -διανυσματικού χώρου (k σώμα) είναι οι υπόχωροι διάστασης 1 και ο τριμμένος υπόχωρος. Τα κυκλικά $\mathbb{Z}$ -υποπρότυπα μιας αβελιανής ομάδας είναι οι κυκλικές υποομάδες της. Ένα παράδειγμα ενός $\mathbb{Z}$ -προτύπου που δεν είναι πεπερασμένα παραγόμενο είναι το $\mathbb{Z}[x]$, τα πολυώνυμα μιας μεταβλητής με ακέραιους συντελεστές (γιατί;). Όμως το $\mathbb{Z}[x]$ είναι πεπερασμένα παραγόμενο $\mathbb{Z}[x]$ -πρότυπο (κάθε δακτύλιος R είναι κυκλικό πρότυπο πάνω από τον εαυτό του, $R = (1_R)$).

Σχόλιο Όλοι οι προηγούμενοι ορισμοί γενικεύουν με φυσικό τρόπο αντίστοιχες έννοιες της Γραμμικής Άλγεβρας. Όμως η δομή R -προτύπων είναι πιο πολύπλοκη από τη δομή k -διανυσματικών χώρων. Αυτό θα γίνει φανερό στο Κεφάλαιο 3 όπου μελετάμε ελεύθερα πρότυπα.

Ασκήσεις 1.1

1. Έστω R ένας δακτύλιος και M μια αβελιανή ομάδα. Δείξτε ότι το M είναι R -πρότυπο αν και μόνο αν υπάρχει ομομορφισμός δακτυλίων $R \rightarrow \text{End} M$.
2. Έστω R ένας μεταθετικός δακτύλιος, M ένα R -πρότυπο, $r \in R$ και $rM = \{rm \mid m \in M\}$. Δείξτε ότι $rM \leq M$ και αν το M είναι πεπερασμένα παραγόμενο, τότε το rM είναι πεπερασμένα παραγόμενο.
3. Αποδείξτε ότι το $\mathbb{Q}$ δεν είναι πεπερασμένα παραγόμενο $\mathbb{Z}$ -πρότυπο.

4. Έστω $\varphi: R \rightarrow S$ ένας ομομορφισμός δακτυλίων και M ένα S -πρότυπο.
 - a. Το M είναι R -πρότυπο με εξωτερικό πολλαπλασιασμό $R \times M \rightarrow M, (r, m) \mapsto \varphi(r)m$.
 - b. Αν το M είναι πεπερασμένα παραγόμενο S -πρότυπο, αληθεύει ότι το M είναι πεπερασμένα παραγόμενο R -πρότυπο;
5. Για $n = 0$ θέτουμε $R_0 = \mathbb{Z}$ και για $n \geq 1$ θέτουμε $R_n = \mathbb{Z}[x_1, \dots, x_n]$, όπου $\mathbb{Z}[x_1, \dots, x_n]$ είναι ο δακτύλιος των πολυωνύμων με ακεραίους συντελεστές στις μεταβλητές $x_1, \dots, x_n$. Έστω $R = \bigcup_{n \geq 0} R_n$. Με τις συνήθεις πράξεις πολυωνύμων, το R είναι ένας δακτύλιος που συνήθως συμβολίζεται με $\mathbb{Z}[x_1, x_2, \dots]$. Να βρεθεί ένα $\mathbb{Z}[x_1, x_2, \dots]$ -υποπρότυπο του $\mathbb{Z}[x_1, x_2, \dots]$ που δεν είναι πεπερασμένα παραγόμενο.
6. Θεωρούμε το $\mathbb{Z}[x]$ ως $\mathbb{Z}[x]$ -πρότυπο. Δείξτε ότι το υποπρότυπο $I = (x, 2) = \{xf(x) + 2g(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}$ του $\mathbb{Z}[x]$ δεν είναι κυκλικό. Συνεπώς γενικά δεν αληθεύει ότι κάθε υποπρότυπο κυκλικού προτύπου είναι κυκλικό.
7. Έστω M μια μη τετριμμένη πεπερασμένη αβελιανή ομάδα. Μπορεί η M να γίνει $\mathbb{Q}$ -διανυσματικός χώρος;
8. Ένα μη μηδενικό R -πρότυπο M λέγεται ανάγωγο αν πέρα από το M και το τετριμμένο πρότυπο, δεν υπάρχουν άλλα υποπρότυπα του M .
 - a. Δείξτε ότι ένα πρότυπο είναι ανάγωγο αν και μόνο είναι παράγεται από κάθε μη μηδενικό στοιχείο του.
 - b. Δείξτε ότι το $\mathbb{Z}_n$ είναι ανάγωγο $\mathbb{Z}$ -πρότυπο αν και μόνο να το n είναι πρώτος.
9. Έστω k ένα σώμα και V ένας k -διανυσματικός χώρος. Δείξτε τα εξής.
 - a. Το σύνολο $\text{End}_k V$ των k -γραμμικών απεικονίσεων $V \rightarrow V$ είναι δακτύλιος με πρόσθεση που ορίζεται από $(f + g)(v) = f(v) + g(v)$ και πολλαπλασιασμό που ορίζεται από $(fg)(v) = f(g(v))$, $f, g \in \text{End}_k V$, $v \in V$.
 - b. Το V είναι ένα $\text{End} V$ πρότυπο με εξωτερικό πολλαπλασιασμό που ορίζεται από $\text{End} V \times V \ni (f, v) \mapsto f(v) \in V$.
 - c. Το V είναι ανάγωγο $\text{End} V$ -πρότυπο (βλ. προηγούμενη άσκηση).

10. Έστω V ένας k -διανυσματικός χώρος, όπου το k είναι σώμα, και $\alpha: V \rightarrow V$ μια γραμμική απεικόνιση. Θεωρούμε το V ως $k[x]$ -πρότυπο (Παράδειγμα 1.1.2 6). Δείξτε ότι αν $\dim V < \infty$, τότε υπάρχει μη μηδενικό $f(x) \in k[x]$ τέτοιο ώστε $f(x)v = 0$ για κάθε $v \in V$.
11. Μια αβελιανή ομάδα M εφοδιάζεται με δομή $\mathbb{Z}_n$ -προτύπου αν και μόνο αν $nx = 0$ για κάθε $x \in M$.

1.2 Ομομορφισμοί Προτύπων

1.2.1 Ορισμός Έστω M, N δυο R -πρότυπα. Μια απεικόνιση $\varphi: M \rightarrow N$ ονομάζεται **ομομορφισμός R -προτύπων** (ή **R -γραμμική**) αν:

- (i) $\varphi(m + m') = \varphi(m) + \varphi(m')$ για κάθε $m, m' \in M$, και
(ii) $\varphi(rm) = r\varphi(m)$ για κάθε $r \in R, m \in M$.

1.2.2 Παραδείγματα

1. Αν M, N είναι R -πρότυπα, η απεικόνιση $M \ni m \mapsto 0 \in N$ είναι ομομορφισμός R -προτύπων (που θα καλούμε **μηδενικό ομομορφισμό**). Η ταυτοτική απεικόνιση $1_M: M \ni m \mapsto m \in M$ είναι επίσης ομομορφισμός R -προτύπων.
2. Αν V και W είναι k -διανυσματικοί χώροι (k σώμα), οι ομομορφισμοί k -προτύπων $V \rightarrow W$ είναι οι k -γραμμικές απεικονίσεις $V \rightarrow W$.
3. Αν G και H είναι δύο αβελιανές ομάδες, οι ομομορφισμοί $\mathbb{Z}$ -προτύπων $G \rightarrow H$ είναι οι ομομορφισμοί ομάδων $G \rightarrow H$.
4. Έστω R ένας δακτύλιος και $a \in R$. Η απεικόνιση $R \ni x \mapsto xa \in R$ είναι ομομορφισμός R -προτύπων. Αντίθετα, η απεικόνιση $R \ni x \mapsto ax \in R$ γενικά δεν είναι ομομορφισμός R -προτύπων (γιατί;).

Ένας ομομορφισμός R -προτύπων $\varphi: M \rightarrow N$ ονομάζεται **επιμορφισμός** (αντίστοιχα **μονομορφισμός**) αν ως απεικόνιση η φ είναι επί (αντίστοιχα 1-1). **Ισομορφισμός R -προτύπων** είναι ένας ομομορφισμός που είναι επί και 1-1. Για παράδειγμα, αν M είναι ένα κυκλικό R -πρότυπο, $M = (m)$, τότε η απεικόνιση $R \rightarrow M, r \mapsto rm$, είναι επιμορφισμός.

Παρατήρηση Έστω $\varphi: L \rightarrow M$ και $\psi: M \rightarrow N$ ομομορφισμοί R -προτύπων. Τότε η σύνθεση $\psi \circ \varphi: L \rightarrow N, a \mapsto \psi(\varphi(a))$ είναι ομομορφισμός R -προτύπων. Επίσης, αν οι φ, ψ είναι ισομορφισμοί, τότε η σύν-

θεση $\psi \circ \varphi$ και οι αντίστροφες απεικονίσεις $\varphi^{-1}: M \rightarrow L$ και $\psi^{-1}: N \rightarrow M$ των φ και ψ αντίστοιχα είναι ισομορφισμοί R -προτύπων. Αφήνουμε τις αποδείξεις ως άσκηση.

Αν M, N είναι R -πρότυπα τέτοια ώστε υπάρχει ισομορφισμός R -προτύπων $M \rightarrow N$, θα λέμε ότι τα M, N είναι **ισόμορφα** και θα το συμβολίζουμε αυτό με $M \simeq N$.

Έστω $\varphi: M \rightarrow N$ ένας ομομορφισμός R -προτύπων. Παρατηρούμε ότι $\varphi(0_M) = 0_N$ αφού $\varphi(0_M) = \varphi(0_M + 0_M) = \varphi(0_M) + \varphi(0_M)$. Από τώρα και στο εξής θα παραλείπουμε τους δείκτες από $0_M, 0_N$ και θα γράφουμε απλά 0 . Ο **πυρήνας** $\ker \varphi$ του φ είναι το σύνολο

$$\ker \varphi = \{a \in M \mid \varphi(a) = 0\}.$$

Το $\ker \varphi$ είναι υποομάδα του M , γιατί φ είναι ομομορφισμός ομάδων. Επιπλέον είναι R -υποπρότυπο του M γιατί για κάθε $r \in R$ και $a \in \ker \varphi$ έχουμε

$$\varphi(a) = 0 \Rightarrow r\varphi(a) = 0 \Rightarrow \varphi(ra) = 0 \Rightarrow ra \in \ker \varphi.$$

Εύκολα βλέπουμε ότι η εικόνα $\operatorname{Im} \varphi$ του φ είναι R -υποπρότυπο του N .

1.2.3 Πρόταση Έστω $\varphi: M \rightarrow N$ ομομορφισμός R -προτύπων. Τότε

- $\ker \varphi \leq M$ και $\operatorname{Im} \varphi \leq N$
- ο φ είναι μονομορφισμός αν και μόνο αν $\ker \varphi = \{0\}$.

Απόδειξη Αν ο φ είναι μονομορφισμός και $m \in \ker \varphi$, τότε από $\varphi(m) = 0 = \varphi(0)$ παίρνουμε $m = 0$. Αντίστροφα, έστω $\ker \varphi = \{0\}$ και $\varphi(m) = \varphi(m')$, $m, m' \in M$. Τότε $\varphi(m - m') = 0 \Rightarrow m - m' = 0 \Rightarrow m = m'$. $\square$

1.2.4 Παρατήρηση Αν $\varphi: M \rightarrow N$ είναι ομομορφισμός R -προτύπων και $L \leq N$, τότε το σύνολο $\varphi^{-1}(L) = \{m \in M \mid \varphi(m) \in L\}$ είναι ένα υποπρότυπο του M που περιέχει το $\ker \varphi$.

Πράγματι, από $0 \in L$ έχουμε $\ker \varphi \subseteq \varphi^{-1}(L)$. Αν $a, b \in \varphi^{-1}(L)$, τότε $\varphi(a), \varphi(b) \in L$ και άρα $\varphi(a - b) = \varphi(a) - \varphi(b) \in L$. Συνεπώς $a - b \in \varphi^{-1}(L)$. Επίσης από $\varphi(ra) = r\varphi(a) \in L$ έπεται ότι $ra \in \varphi^{-1}(L)$.

Έστω M ένα R -πρότυπο και $N \leq M$. Θεωρώντας τα M, N ως αβελιανές ομάδες, ξέρουμε ότι το πηλίκο

$$M/N = \{a + N \mid a \in M\}$$

είναι αβελιανή ομάδα με πρόσθεση $(a + N) + (b + N) = (a + b) + N$. Η M/N γίνεται R -πρότυπο με εξωτερικό πολλαπλασιασμό

$$R \times M/N \rightarrow M/N, (r, a + N) \mapsto r(a + N) = ra + N.$$

Η απεικόνιση αυτή είναι καλά ορισμένη γιατί αν $a + N = a' + N$, τότε $a - a' \in N \Rightarrow ra - ra' = r(a - a') \in N \Rightarrow ra + N = ra' + N$.

Τώρα η επαλήθευση των ιδιοτήτων του Ορισμού 1.1.1 είναι άμεση. Το R -πρότυπο M/N ονομάζεται το R -πρότυπο **πηλίκο** του M modulo N . Η απεικόνιση $M \rightarrow M/N, m \mapsto m + N$, είναι ένας επιμορφισμός προτύπων που θα ονομάζουμε **φυσικό επιμορφισμό** ή **φυσική προβολή**.

1.2.5 Πρόταση Έστω M ένα R -πρότυπο και $N \leq M$. Τότε κάθε υποπρότυπο του M/N είναι της μορφής L/N , όπου $N \leq L \leq M$.

Απόδειξη Αν $\varphi: M \rightarrow M/N$ είναι ο φυσικός επιμορφισμός και $A \leq M/N$, τότε από την Παρατήρηση 1.2.4, το $\varphi^{-1}(A)$ είναι ένα υποπρότυπο του M που περιέχει το $\ker \varphi = N$. Ισχύει $\varphi(\varphi^{-1}(A)) = A$. $\square$

Κατ' αναλογία με τους διανυσματικούς χώρους, τις αβελιανές ομάδες και τα ιδεώδη, υπάρχουν και εδώ θεωρήματα ισομορφισμών. Χρειαζόμαστε έναν ορισμό. Έστω M ένα R -πρότυπο και A, B υποπρότυπα του M . Με $A + B$ συμβολίζουμε το υποπρότυπο του M που παράγεται από το υποσύνολο $A \cup B$. Φυσικά ισχύει $A + B = \{a + b \in M \mid a \in A, b \in B\}$. Παρατηρούμε ότι $A \leq A + B$ και $B \leq A + B$.

Παράδειγμα Αν $m, n \in \mathbb{N}$ και $\mu\kappa\delta(m, n) = d$, τότε $\mathbb{Z}m + \mathbb{Z}n = \mathbb{Z}d$.

Πράγματι, επειδή $d \mid m$ έχουμε $\mathbb{Z}m \subseteq \mathbb{Z}d$. Όμοια $\mathbb{Z}n \subseteq \mathbb{Z}d$ και άρα $\mathbb{Z}m + \mathbb{Z}n \subseteq \mathbb{Z}d$. Επειδή $\mu\kappa\delta(m, n) = d$, υπάρχουν $x, y \in \mathbb{Z}$ με $d = xm + yn$. Άρα $d \in \mathbb{Z}m + \mathbb{Z}n$ και συνεπώς $\mathbb{Z}d \subseteq \mathbb{Z}m + \mathbb{Z}n$.

1.2.7 Θεώρημα (Θεωρήματα Ισομορφισμών Προτύπων)

1°. Έστω $\varphi: M \rightarrow N$ ένας ομομορφισμός R -προτύπων. Τότε η απεικόνιση

$$\bar{\varphi}: M/\ker \varphi \ni m + \ker \varphi \mapsto \varphi(m) \in \operatorname{Im} \varphi$$

είναι ισομορφισμός R -προτύπων.

2°. Έστω ότι A, B είναι R -υποπρότυπα του R -προτύπου M . Τότε υπάρχει ισομορφισμός R -προτύπων

$$(A + B)/A \simeq B/A \cap B.$$

3°. Έστω $C \leq B \leq A$ R -πρότυπα. Τότε υπάρχει ισομορφισμός R -προτύπων

$$(A/C)/(B/C) \simeq A/B.$$

Απόδειξη 1. Η $\bar{\varphi}$ είναι καλά ορισμένη γιατί αν $m + \ker \varphi = m' + \ker \varphi$, τότε $m - m' \in \ker \varphi \Rightarrow \varphi(m - m') = 0 \Rightarrow \varphi(m) = \varphi(m')$. Η $\bar{\varphi}$ είναι ομομορφισμός R -προτύπων γιατί αν $m, m' \in M, r \in R$ έχουμε

$$\bar{\varphi}((m + \ker \varphi) + (m' + \ker \varphi)) = \bar{\varphi}(m + m' + \ker \varphi) =$$

$$\varphi(m + m') = \varphi(m) + \varphi(m') = \bar{\varphi}(m + \ker \varphi) + \bar{\varphi}(m' + \ker \varphi)$$

και

$$\bar{\varphi}(r(m + \ker \varphi)) = \bar{\varphi}(rm + \ker \varphi) = \varphi(rm) =$$

$$r\varphi(m) = r\bar{\varphi}(m + \ker \varphi).$$

Η $\bar{\varphi}$ είναι 1-1 γιατί αν $\bar{\varphi}(m + \ker \varphi) = \bar{\varphi}(m' + \ker \varphi)$, τότε $\varphi(m) = \varphi(m')$, οπότε $m - m' \in \ker \varphi$, δηλαδή $m + \ker \varphi = m' + \ker \varphi$. Τέλος, είναι σαφές από τον ορισμό ότι η $\bar{\varphi}$ είναι επί.

2. Η απεικόνιση

$$\varphi: B \rightarrow (A + B)/A, \varphi(b) = b + A$$

είναι επιμορφισμός R -προτύπων και $\ker \varphi = \{b \in B \mid b + A = 0\} = A \cap B$.

Άρα από το 1^ο Θεώρημα Ισομορφισμών Προτύπων προκύπτει $B/A \cap B \cong (A + B)/A$.

3. Εφόσον $C \subseteq B$ η απεικόνιση

$$\varphi: A/C \rightarrow A/B, \varphi(a + C) = a + B$$

είναι ένας καλά ορισμένος επιμορφισμός R -προτύπων. Ισχύει $\ker \varphi = \{a + C \mid a + B = 0\} = B/C$. Από το 1^ο Θεώρημα Ισομορφισμών R -προτύπων προκύπτει το ζητούμενο. $\square$

Έστω M ένα R -πρότυπο. Το σύνολο

$$\text{Ann } M = \{r \in R \mid rm = 0 \text{ για κάθε } m \in M\}$$

είναι ιδεώδες του R . Πράγματι, (i) $\text{Ann } M \neq \emptyset$ αφού $0 \in \text{Ann } M$, (ii) $r, s \in \text{Ann } M \Rightarrow (r + s)m = rm + sm = 0$ για κάθε $m \in M$ και άρα $r + s \in \text{Ann } M$, και (iii) $x \in R, r \in \text{Ann } M \Rightarrow (xr)m = x(rm) = 0$ για κάθε $m \in M$ και άρα $xr \in \text{Ann } M$. Το ιδεώδες $\text{Ann } M$ ονομάζεται ο **μηδενιστής** (ή η **τάξη**) του M . Για παράδειγμα, αν το V είναι ένας μη τετριμμένος k -διανυσματικός χώρος, τότε $\text{Ann } V = \{0\}$. Για το $\mathbb{Z}$ -πρότυπο $\mathbb{Z}_n$ ισχύει $\text{Ann } \mathbb{Z}_n = n\mathbb{Z}$. Για το $\mathbb{Z}_n$ -πρότυπο $\mathbb{Z}_n$ ισχύει $\text{Ann } \mathbb{Z}_n = \{[0]\}$.

Αν $m \in M$, θέτουμε $\text{Ann}(m) = \{r \in R \mid rm = 0\}$. Το $\text{Ann}(m)$ είναι ιδεώδες του R που ονομάζεται ο **μηδενιστής** (ή η **τάξη**) του m . Παρατηρούμε ότι $\text{Ann } M = \bigcap_{m \in M} \text{Ann}(m)$. Σημειώνουμε ότι αν ο R δεν είναι με-

ταθετικός, ενδέχεται να ισχύει $\text{Ann}(m) \neq \text{Ann}((m))$, όπου $\text{Ann}((m))$ είναι ο μηδενιστής του κυκλικού προτύπου (m) , βλ. Άσκηση 4.

Η επόμενη πρόταση μας πληροφορεί ότι πάνω από μεταθετικούς δακτύλιους, κυκλικά πρότυπα καθορίζονται από τους μηδενιστές τους.

1.2.8 Πρόταση Έστω R ένας μεταθετικός δακτύλιος και M ένα R -πρότυπο. Τότε το M είναι κυκλικό αν και μόνο αν $M \simeq R/\text{Ann}M$. Επιπλέον, δυο κυκλικά R -πρότυπα M, N είναι ισόμορφα αν και μόνο αν $\text{Ann}M = \text{Ann}N$.

Απόδειξη Έστω ότι το M είναι κυκλικό, $M = (m)$. Η απεικόνιση $R \rightarrow M, r \mapsto rm$ είναι ένας επιμορφισμός R -προτύπων και ο πυρήνας είναι το $\{r \in R \mid rm = 0\} = \text{Ann}(m)$ που ισούται με το $\text{Ann}M$ (γιατί ο R είναι μεταθετικός). Από το 1^ο Θεώρημα Ισομορφισμών Προτύπων υπάρχει ισομορφισμός προτύπων $R/\text{Ann}M \simeq M$. Αντίστροφα, αν $M \simeq R/\text{Ann}M$, τότε το M είναι κυκλικό αφού το $R/\text{Ann}M$ παράγεται από το στοιχείο $1 + \text{Ann}M$.

Έστω ότι τα πρότυπα M, N είναι κυκλικά. Αν $\text{Ann}M = \text{Ann}N$, τότε $M \simeq R/\text{Ann}M = R/\text{Ann}N \simeq N$. Αντίστροφα, αν $M \simeq N$, τότε έχουμε $\text{Ann}M = \text{Ann}N$ σύμφωνα με την Άσκηση 1. $\square$

Άσκησης 1.2

1. Αν τα R -πρότυπα M, N είναι ισόμορφα, τότε $\text{Ann}M = \text{Ann}N$. Αληθεύει το αντίστροφο;
2. Δείξτε ότι αν $f: M \rightarrow N$ ένας ομομορφισμός R προτύπων, όπου το M είναι κυκλικό, $M = (m)$, τότε ο f καθορίζεται από την εικόνα $f(m)$. Να βρεθούν οι ομομορφισμοί $\mathbb{Z}$ -προτύπων $\mathbb{Z} \rightarrow \mathbb{Z}$, οι ισομομορφισμοί $\mathbb{Z}$ -προτύπων $\mathbb{Z} \rightarrow \mathbb{Z}$, οι ομομορφισμοί $\mathbb{Z}$ -προτύπων $\mathbb{Z}_n \rightarrow \mathbb{Z}$.
3. Έστω R μια περιοχή $r \in R, r \neq 0$, και $n \in \mathbb{N}$.
 - a. Δείξτε ότι η απεικόνιση $R \rightarrow Rr^n, x \mapsto xr^n$, είναι επιμορφισμός R -προτύπων.
 - b. Δείξτε ότι υπάρχει ισομορφισμός R -προτύπων $R/Rr \simeq Rr^n/Rr^{n+1}$.

4. Έστω $M_2(R)$ ο δακτύλιος των 2×2 πινάκων με στοιχεία από ένα δακτύλιο R . Η αβελιανή ομάδα $M = M_{2 \times 1}(R)$ είναι $M_2(R)$ -πρότυπο (βλ. Παράδειγμα 1.1.2 8). Έστω $m = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.
- Δείξτε ότι $M = (m)$.
 - Δείξτε ότι $\text{Ann}M = 0$ και $\text{Ann}(m) \neq 0$.
5. Έστω $\varphi: M \rightarrow M$ ένας ομομορφισμός R -προτύπων. Δείξτε ότι $M = \ker \varphi + \text{Im} \varphi \Leftrightarrow \text{Im} \varphi = \text{Im} \varphi^2$ (όπου με φ^2 συμβολίζουμε τη σύνθεση $\varphi \circ \varphi$).
6. Έστω M ένα R -πρότυπο και $A, B, C \leq M$.
- Δείξτε ότι $A \cap (B + C) \supseteq A \cap B + A \cap C$
 - Αληθεύει ότι $A \cap (B + C) = A \cap B + A \cap C$;
 - Δείξτε ότι αν $C \leq A$, τότε $A \cap (B + C) = A \cap B + C$.
7. Έστω M ένα R -πρότυπο.
- Έστω $N \leq M$ τέτοιο ώστε το N και το M/N είναι πεπερασμένα παραγόμενα. Δείξτε ότι το M είναι πεπερασμένα παραγόμενο.
 - Έστω $L, N \leq M$. Δείξτε ότι αν τα $L + N, L \cap N$ είναι πεπερασμένα παραγόμενα, τότε και τα L, N είναι πεπερασμένα παραγόμενα.
8. Έστω I ιδεώδες του R . Αν M είναι ένα R -πρότυπο, ορίζουμε IM ως το υποπρότυπο του M που παράγεται από το σύνολο $\{am \mid a \in I, m \in M\}$. Τότε το M/IM είναι R/I -πρότυπο με εξωτερικό πολλαπλασιασμό που ορίζεται από $(r + I)(m + IM) = rm + IM$.
9. Έστω p πρώτος αριθμός και M μια πεπερασμένη αβελιανή ομάδα τέτοια ώστε $pm = 0$ για κάθε $m \in M$. Δείξτε ότι η M είναι $\mathbb{Z}_p$ -διανυσματικός χώρος και $|M| = p^n$.
10. Έστω M ένα ανάγωγο R -πρότυπο (βλ. Άσκηση 1.1.8). Δείξτε ότι κάθε μη μηδενικός ομομορφισμός R -προτύπων $M \rightarrow M$ είναι ισομορφισμός.
11. Έστω k ένα σώμα και V ένας k -διανυσματικός χώρος με $\dim V = n < \infty$.
- Αν $U \leq V$, δείξτε ότι $\dim \frac{V}{U} = \dim V - \dim U$.

- b. Αν $U, W \leq V$, δείξτε χρησιμοποιώντας το 2^ο Θεώρημα Ισομορφισμών Προτύπων ότι
- $$\dim(U + W) = \dim U + \dim W - \dim U \cap W.$$

1.3 Αθροίσματα Προτύπων

Αν $M_1, \dots, M_n$ είναι R -πρότυπα, τότε το σύνολο των διατεταγμένων n -άδων $M_1 \times \dots \times M_n = \{(x_1, \dots, x_n) \mid x_i \in M_i, i = 1, \dots, n\}$, είναι ένα R -πρότυπο με πρόσθεση και εξωτερικό πολλαπλασιασμό που ορίζονται αντίστοιχα από τις σχέσεις

$$(x_1, \dots, x_n) + (x_1', \dots, x_n') = (x_1 + x_1', \dots, x_n + x_n'),$$

$$r(x_1, \dots, x_n) = (rx_1, \dots, rx_n).$$

Θα το ονομάζουμε το **εξωτερικό ευθύ άθροισμα** των $M_1, \dots, M_n$.

Έστω M ένα R -πρότυπο και $M_1, \dots, M_n$ υποπρότυπα του M . Θα λέμε ότι το M είναι το **εσωτερικό ευθύ άθροισμα** των $M_1, \dots, M_n$ αν κάθε $m \in M$ γράφεται κατά μοναδικό τρόπο ως άθροισμα της μορφής $m = m_1 + \dots + m_n$, με $m_i \in M_i$ για κάθε $i = 1, \dots, n$. Στην περίπτωση αυτή θα γράφουμε $M = M_1 \oplus \dots \oplus M_n$.

Παρατηρούμε ότι αν M είναι ένα R -πρότυπο και $M_1, \dots, M_n$ υποπρότυπα του M , τότε το **εξωτερικό ευθύ άθροισμα** των $M_1, \dots, M_n$ ορίζεται, αλλά το **εσωτερικό ευθύ άθροισμα** των $M_1, \dots, M_n$ ενδέχεται να μην ορίζεται. Η επόμενη πρόταση παρέχει ένα κριτήριο για το εσωτερικό ευθύ άθροισμα.

Αν $M_1, \dots, M_n$ είναι υποπρότυπα ενός R -προτύπου M , με $\sum_{i=1}^n M_i$ ή $M_1 + \dots + M_n$ συμβολίζουμε το R -υποπρότυπο του M που παράγεται από το σύνολο $M_1 \cup \dots \cup M_n$. Παρατηρούμε ότι

$$\sum_{i=1}^n M_i = \{m_1 + \dots + m_n \mid m_i \in M_i, i = 1, \dots, n\}.$$

1.3.1 Πρόταση Έστω $M_1, \dots, M_n$ υποπρότυπα ενός R -προτύπου M . Τότε $M = M_1 \oplus \dots \oplus M_n$ αν και μόνο αν

- (i) $M = \sum_{i=1}^n M_i$ και
(ii) για κάθε $i = 1, \dots, n$, $M_i \cap \sum_{j \neq i} M_j = 0$.

Απόδειξη Αν $m \in M$ και $m = m_1 + \dots + m_n = m_1' + \dots + m_n'$ με $m_i, m_i' \in M_i$, τότε

$$M_i \ni m_i - m_i' = \sum_{j \neq i} (m_j' - m_j) \in \sum_{j \neq i} M_j.$$

Τώρα αν ισχύει η συνθήκη (ii) παίρνουμε $m_i = m_i'$. Συνεπώς, αν ισχύουν οι συνθήκες της πρότασης, έχουμε $M = M_1 \oplus \dots \oplus M_n$. Αντίστροφα, αν κάθε $m \in M$ έχει μοναδική γραφή της μορφής $m = m_1 + \dots + m_n$, $m_i \in M_i$, τότε ισχύει προφανώς η συνθήκη (i). Αλλά και η συνθήκη (ii) ισχύει, γιατί αν $M_i \cap \sum_{j \neq i} M_j \neq 0$, θα είχαμε μια ισότητα της μορφής $m_i = \sum_{j \neq i} m_j$, όπου $m_t \in M_t$, $t = 1, \dots, n$, και $m_i \neq 0$. Δηλαδή θα είχαμε δύο διαφορετικές παραστάσεις για το m_i . $\square$

Έστω ότι M είναι ένα R -πρότυπο τέτοιο ώστε $M = M_1 \oplus M_2$. Επειδή κάθε $m \in M$ γράφεται μοναδικά στη μορφή $m = m_1 + m_2$, $m_i \in M_i$, η απεικόνιση $M \rightarrow M_1, m \mapsto m_1$ είναι καλά ορισμένη. Είναι επιμορφισμός προτύπων με πυρήνα το M_2 . Από το 1^ο Θεώρημα Ισομορφισμών Προτύπων έχουμε $M/M_2 \simeq M_1$. Με όμοιο τρόπο αποδεικνύεται η εξής πρόταση της οποίας η απόδειξη αφήνεται ως άσκηση.

1.3.2 Πρόταση Αν $M = M_1 \oplus \dots \oplus M_n$, τότε για κάθε i

$$M_i \simeq \frac{M}{M_1 + \dots + \widehat{M_i} + \dots + M_n},$$

όπου $\widehat{M_i}$ σημαίνει ότι παραλείπεται ο όρος M_i .

Παρατήρηση στο συμβολισμό

Έστω ότι $M_1, \dots, M_n$ είναι R -πρότυπα και $M = M_1 \times \dots \times M_n$. Θέτοντας $\overline{M_i} = \{(0_{M_1}, \dots, m_i, \dots, 0_{M_n}) \in M \mid m_i \in M_i\}$, όπου το m_i βρίσκεται στην i συντεταγμένη, εύκολα αποδεικνύεται ότι $M = \overline{M_1} \oplus \dots \oplus \overline{M_n}$ και επιπλέον για κάθε i έχουμε $\overline{M_i} \simeq M_i$. Δηλαδή, το εσωτερικό ευθύ άθροισμα

$\overline{M_1} \oplus \dots \oplus \overline{M_n}$ είναι ίσο με το εξωτερικό ευθύ άθροισμα $M_1 \times \dots \times M_n$ και για κάθε i έχουμε $\overline{M_i} \simeq M_i$. Λαμβάνοντας υπόψη την παρατήρηση αυτή, από τώρα και στο εξής θα χρησιμοποιούμε το συμβολισμό $M_1 \oplus \dots \oplus M_n$ και για το εξωτερικό ευθύ άθροισμα $M_1 \times \dots \times M_n$ (που ορίζεται πάντοτε) και για το εσωτερικό ευθύ άθροισμα (όταν ορίζεται). Από τα συμφραζόμενα μιας διατύπωσης θα είναι σαφές ποια περίπτωση ισχύει.

1.3.3 Παραδείγματα

1. Έστω m, n δυο θετικοί ακέραιοι με $\mu\kappa\delta(m, n) = 1$. Τότε υπάρχει ισομορφισμός $\mathbb{Z}$ -προτύπων $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \oplus \mathbb{Z}_n$.

Πράγματι, ορίζουμε την αντιστοιχία

$$f : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \oplus \mathbb{Z}_n, [a]_{mn} \mapsto ([a]_m, [a]_n)$$

και παρατηρούμε ότι αυτή είναι απεικόνιση γιατί αν $[a]_{mn} = [b]_{mn}$, τότε το mn διαιρεί το $a - b$, $mn | a - b$, και επομένως $m | a - b$ και $n | a - b$, δηλαδή $[a]_m = [b]_m$ και $[a]_n = [b]_n$. Η f είναι ομομορφισμός $\mathbb{Z}$ -προτύπων αφού για κάθε $[a]_{mn}, [b]_{mn} \in \mathbb{Z}_{mn}, r \in \mathbb{Z}$ έχουμε

$$\begin{aligned} f([a]_{mn} + [b]_{mn}) &= f([a + b]_{mn}) = ([a + b]_m, [a + b]_n) = \\ &= ([a]_m, [a]_n) + ([b]_m, [b]_n) = f([a]_{mn}) + f([b]_{mn}) \end{aligned}$$

και

$$f(r[a]_{mn}) = f([ra]_{mn}) = ([ra]_m, [ra]_n) = r([a]_m, [a]_n) = rf([a]_{mn}).$$

Παρατηρούμε ότι ο ομομορφισμός f είναι 1-1 γιατί αν $[a]_{mn} \in \ker f$, τότε $f([a]_{mn}) = ([0]_m, [0]_n) \Rightarrow [a]_m = [0]_m, [a]_n = [0]_n$ και άρα $m | a$ και $n | a$. Επειδή $\mu\kappa\delta(m, n) = 1$, παίρνουμε $mn | a$, δηλαδή $[a]_{mn} = [0]_{mn}$ και συνεπώς $\ker f = \{[0]_{mn}\}$. Επειδή τα πεπερασμένα σύνολα $\mathbb{Z}_{mn}, \mathbb{Z}_m \oplus \mathbb{Z}_n$ έχουν το αυτό πλήθος στοιχείων και η απεικόνιση $f : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \oplus \mathbb{Z}_n$ είναι 1-1, συμπεραίνουμε ότι η f είναι και επί. Τελικά η f είναι ισομορφισμός $\mathbb{Z}$ -προτύπων.

Σημείωση. Με μια εύκολη επαγωγή αποδεικνύεται ότι για κάθε $n \in \mathbb{N}$ υπάρχει ισομορφισμός $\mathbb{Z}$ -προτύπων

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{n_1}} \oplus \dots \oplus \mathbb{Z}_{p_k^{n_k}}$$

όπου $n = p_1^{n_1} \dots p_k^{n_k}$ είναι η ανάλυση του n σε γινόμενο πρώτων ($p_1, \dots, p_k$ είναι διακεκριμένοι πρώτοι αριθμοί).

2. Έστω M ένα R -πρότυπο και $f: M \rightarrow M$ ένας ομομορφισμός R -προτύπων τέτοιος ώστε $f = f^2$, όπου με f^2 συμβολίζουμε τη σύνθεση $f \circ f$. Τότε $M = \ker f \oplus \operatorname{Im} f$.

Πράγματι, έστω $m \in M$. Γράφοντας $m = (m - f(m)) + f(m)$ παρατηρούμε ότι $m - f(m) \in \ker f$, γιατί $f(m - f(m)) = f(m) - f^2(m) = 0$, και συνεπώς $M \subseteq \ker f + \operatorname{Im} f$. Άρα έχουμε $M = \ker f + \operatorname{Im} f$. Αν $a \in \ker f \cap \operatorname{Im} f$, τότε αφενός $f(a) = 0$ και αφετέρου $a = f(b)$ για κάποιο $b \in M$. Άρα $0 = f(a) = f^2(b) = f(b) = a$, δηλαδή $\ker f \cap \operatorname{Im} f = 0$. Από την Πρόταση 1.3.1 προκύπτει το ζητούμενο.

Ας δούμε τώρα συνοπτικά τη σχέση αθροισμάτων προτύπων με πεπερασμένα παραγόμενα πρότυπα.

1.3.4 Πρόταση Έστω M ένα R -πρότυπο και $M_1, \dots, M_n \leq M$.

- (i) Αν $M = M_1 + \dots + M_n$ και κάθε M_i είναι πεπερασμένα παραγόμενο, τότε το M είναι πεπερασμένα παραγόμενο.
- (ii) Αν το M είναι πεπερασμένα παραγόμενο και $N \leq M$, τότε το M/N είναι πεπερασμένα παραγόμενο.
- (iii) Αν $M = M_1 \oplus \dots \oplus M_k$ και το M είναι πεπερασμένα παραγόμενο, τότε κάθε M_i είναι πεπερασμένα παραγόμενο.

Απόδειξη (i) Έστω ότι το M_i παράγεται από το πεπερασμένο σύνολο X_i , $i = 1, \dots, n$. Τότε το M παράγεται από το σύνολο $X_1 \cup \dots \cup X_n$ που είναι πεπερασμένο.

(ii) Αν το M παράγεται από τα στοιχεία $m_1, \dots, m_s$, τότε το M/N παράγεται από τα στοιχεία $m_1 + N, \dots, m_s + N$.

(iii) Αυτό έπεται άμεσα από το (ii) και την Πρόταση 1.3.2. $\square$

Ένα υποπρότυπο M_1 του M λέγεται **ευθύς προσθετός** του M αν υπάρχει $M_2 \leq M$ τέτοιο ώστε $M = M_1 \oplus M_2$. Στην προηγούμενη πρόταση είδαμε ότι κάθε ευθύς προσθετός πεπερασμένα παραγόμενου προτύπου είναι πεπερασμένα παραγόμενο πρότυπο. Επισημαίνουμε ότι τυχαίο υποπρότυπο πεπερασμένα παραγόμενου προτύπου δεν είναι αναγκαστικά πεπερασμένα παραγόμενο. Ακολουθεί σχετικό παράδειγμα.

Παράδειγμα Έστω R ο δακτύλιος των συναρτήσεων $\mathbb{R} \rightarrow \mathbb{R}$ με πρόσθεση και πολλαπλασιασμό που ορίζονται από τις σχέσεις

$$(f + g)(x) = f(x) + g(x)$$

$$(fg)(x) = f(x)g(x),$$

όπου $f, g \in R, x \in \mathbb{R}$. Ως R -πρότυπο, το R είναι πεπερασμένα παραγόμενο (πχ από τη συνάρτηση $\mathbb{R} \rightarrow \mathbb{R}, x \mapsto 1$, η οποία είναι το μοναδιαίο στοιχείο του δακτυλίου R). Θεωρούμε το σύνολο

$$I = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid \exists n \in \mathbb{N}, f(x) = 0 \forall x \notin [-n, n]\},$$

δηλαδή το σύνολο των συναρτήσεων $\mathbb{R} \rightarrow \mathbb{R}$ που είναι μηδέν στο συμπλήρωμα κάποιου κλειστού διαστήματος της μορφής $[-n, n]$. Είναι σαφές ότι το I είναι ένα R -υποπρότυπο του R . Θα δείξουμε ότι το I δεν είναι πεπερασμένα παραγόμενο.

Έστω ότι το I είναι πεπερασμένα παραγόμενο, $I = (f_1, \dots, f_k)$. Τότε κάθε στοιχείο του I γράφεται ως $g_1 f_1 + \dots + g_k f_k$, όπου $g_i \in R$. Υπάρχουν $n_i \in \mathbb{N}$ με $f_i(x) = 0 \forall x \notin [-n_i, n_i]$, $i = 1, \dots, k$. Επιλέγοντας $n = \max\{n_i\}$, βλέπουμε ότι κάθε f_i είναι μηδέν στο συμπλήρωμα του διαστήματος $[-n, n]$ και άρα η συνάρτηση $g_1 f_1 + \dots + g_k f_k$ έχει την ιδιότητα αυτή. Συνεπώς κάθε συνάρτηση στο I είναι μηδέν στο συμπλήρωμα του διαστήματος $[-n, n]$. Όμως, η συνάρτηση

$$\mathbb{R} \rightarrow \mathbb{R}, x \mapsto \begin{cases} 0, & x \notin [-(n+1), n+1] \\ 1, & x \in [-(n+1), n+1] \end{cases}$$

ανήκει στο I αλλά δεν είναι μηδέν στο συμπλήρωμα του διαστήματος $[-n, n]$, πράγμα άτοπο.

Ασκήσεις 1.3

1. Έστω M ένα R -πρότυπο και $M_1, M_2 \leq M$ τέτοια ώστε $M = M_1 \oplus M_2$. Δείξτε ότι αν το M είναι κυκλικό, τότε τα M_i είναι κυκλικά. Δείξτε με παράδειγμα ότι το αντίστροφο δεν ισχύει.
2. Θεωρούμε το δακτύλιο $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Z}\}$ (με τις συνήθεις πράξεις πραγματικών αριθμών).
 - a. Αποδείξτε ότι υπάρχει ισομορφισμός $\mathbb{Z}$ -προτύπων $\mathbb{Z}[\sqrt{2}] \simeq \mathbb{Z} \oplus \mathbb{Z}$, αλλά δεν υπάρχει ισομορφισμός δακτυλίων $\mathbb{Z}[\sqrt{2}] \rightarrow \mathbb{Z} \oplus \mathbb{Z}$.
 - b. Βρείτε $\mathbb{Z}$ -υποπρότυπα $M, N \leq \mathbb{Z}[\sqrt{2}]$ τέτοια ώστε $\mathbb{Z}[\sqrt{2}] = M \oplus N$, $M \simeq \mathbb{Z}$, $N \simeq \mathbb{Z}$ και $M, N \neq \mathbb{Z}$.

3. Έστω R μια περιοχή. Δείξτε ότι δεν υπάρχουν μη μηδενικά ιδεώδη I, J του R τέτοια ώστε $R = I \oplus J$.
4. Αποδείξτε ότι υπάρχει ισομορφισμός R -προτύπων $M_2(R) \simeq R \oplus R \oplus R \oplus R$, όπου $M_2(R)$ είναι το R -πρότυπο των 2×2 πινάκων με στοιχεία από το R .
5. Έστω A, B, C, D R -πρότυπα. Δείξτε ότι αν $A \simeq C$ και $B \simeq D$, τότε $A \oplus B \simeq C \oplus D$.
6. Έστω M ένα R -πρότυπο, $r \in R$ ένα αντιστρέψιμο στοιχείο και $\varphi: M \rightarrow M$ ένας ομομορφισμός R -προτύπων για τον οποίο ισχύει $\varphi^2 = r\varphi$. Αποδείξτε ότι $M = \ker \varphi \oplus \operatorname{Im} \varphi$.
7. Θεωρούμε τη γραμμική απεικόνιση $\varphi: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ που, ως προς τη συνήθη βάση του $\mathbb{R}^3$, έχει πίνακα τον $\begin{pmatrix} 5 & -10 & 5 \\ -2 & 6 & 2 \\ 1 & 2 & 9 \end{pmatrix}$. Αποδείξτε ότι $\mathbb{R}^3 = \ker \varphi \oplus \operatorname{Im} \varphi$ με δυο διαφορετικούς τρόπους α) χρησιμοποιώντας την προηγούμενη άσκηση β) χρησιμοποιώντας την έννοια των διαγωνίσιμων πινάκων από τη Γραμμική Άλγεβρα.
8. Έστω R ένας μεταθετικός δακτύλιος και M ένα R -πρότυπο. Αν $r \in R$, θέτουμε $rM = \{rm \mid m \in M\}$, $M_r = \{m \in M \mid rm = 0\}$.
 - a. Δείξτε ότι $rM \leq M$, $M_r \leq M$ και $M/M_r \simeq rM$.
 - b. Αν $M_1, M_2 \leq M$ με $M = M_1 \oplus M_2$, δείξτε ότι $rM = rM_1 \oplus rM_2$ και $M_r = (M_1)_r \oplus (M_2)_r$.
 - c. Έστω $R = \mathbb{Z}$ και a, b δυο ακέραιοι τέτοιοι ώστε $\mu\kappa\delta(a, b) = 1$. Αν M είναι ένα $\mathbb{Z}$ -πρότυπο τέτοιο ώστε $abM = 0$, δείξτε ότι $M = M_a \oplus M_b$.
9. Έστω M ένα R -πρότυπο και $M_1, M_2 \leq M$ τέτοια ώστε $M = M_1 \oplus M_2$. Αν $N \leq M$ με $M_1 \subseteq N$, δείξτε ότι $N = M_1 \oplus (N \cap M_2)$.
10. Έστω M ένα R -πρότυπο και $M_1, \dots, M_n \leq M$ τέτοια ώστε $M = M_1 \oplus \dots \oplus M_k$. Έστω $N_1 \leq M_1, \dots, N_k \leq M_k$ και $N = N_1 + \dots + N_k$. Αποδείξτε τα εξής.
 - a. $N = N_1 \oplus \dots \oplus N_k$.
 - b. $M/N = \pi(M_1) \oplus \dots \oplus \pi(M_k)$, όπου $\pi: M \rightarrow M/N$ είναι ο φυσικός επιμορφισμός.
 - c. $M/N \simeq M_1/N_1 \oplus \dots \oplus M_k/N_k$.

11. Έστω U, V δυο k - διανυσματικοί χώροι, όπου το k είναι σώμα, και $\alpha: U \rightarrow U$, $\beta: V \rightarrow V$ γραμμικές απεικονίσεις. Θεωρούμε τα U, V ως $k[x]$ -πρότυπα (Παράδειγμα 1.1.2 6). Δείξτε ότι $U \simeq V$ ως $k[x]$ -πρότυπα αν και μόνο αν υπάρχει ισομορφισμός διανυσματικών χώρων $\varphi: U \rightarrow V$ τέτοιος ώστε $\alpha = \varphi^{-1}\beta\varphi$.
12. Έστω $M = M_{n \times 1}(R)$ η αβελιανή ομάδα των $n \times 1$ πινάκων με στοιχεία από το δακτύλιο R . Με τον πολλαπλασιασμό πινάκων, το M είναι ένα $M_n(R)$ -πρότυπο (βλ. Παράδειγμα 1.1.2 8). Δείξτε ότι υπάρχει ισομορφισμός $M_n(R)$ -προτύπων $M_n(R) \simeq M \oplus \dots \oplus M$ (n φορές).
13. Εξετάστε αν η ακόλουθη πρόταση είναι σωστή. Έστω M ένα R -πρότυπο και $M_1, \dots, M_n \leq M$ τέτοια ώστε $M = M_1 + \dots + M_n$. Ισχύει $M = M_1 \oplus \dots \oplus M_n$ αν

$$M_1 \cap M_2 = 0$$

$$(M_1 + M_2) \cap M_3 = 0$$

$$\vdots$$

$$(M_1 + \dots + M_{n-1}) \cap M_n = 0.$$